

A Critical Evaluation of Webblocking Injunctions Viewed From Two Perspectives: Effectiveness and Legitimacy

Hyland, Mark

Law, Innovation and Technology

DOI:

[10.1080/17579961.2020.1727058](https://doi.org/10.1080/17579961.2020.1727058)

Published: 31/03/2020

Peer reviewed version

[Cyswllt i'r cyhoeddiad / Link to publication](https://doi.org/10.1080/17579961.2020.1727058)

Dyfyniad o'r fersiwn a gyhoeddwyd / Citation for published version (APA):

Hyland, M. (2020). A Critical Evaluation of Webblocking Injunctions Viewed From Two Perspectives: Effectiveness and Legitimacy. *Law, Innovation and Technology*.
<https://doi.org/10.1080/17579961.2020.1727058>

Hawliau Cyffredinol / General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

A critical evaluation of webblocking Injunctions from the perspectives of effectiveness and legitimacy¹

M.Hylland

1. Introduction

A webblocking order² is, in effect, an order granted in favour of one or more IP rightsholders and against one or more ISPs, requiring the Defendant ISPs to block or attempt to block access by internet users to one or more websites which facilitate IP infringement.³ This article will critically evaluate the increasingly popular webblocking injunction in the online environment and assess the extent to which it addresses two distinct concerns, firstly, effectiveness,⁴ and, secondly, legitimacy.⁵ This critical evaluation will primarily assess webblocking injunctions in the context of court judgments (principally UK, and CJEU), but will also include empirical studies and commentary from both legal academics and practising lawyers.⁶

¹ The author would like to express his thanks to Professor Dermot Cahill, Head of Bangor University Law School, for his very valuable comments and observations during the writing of this article. All errors and omissions remain mine alone.

² Sometimes referred to by the author as “a webblock” or, a “blocking order”, or “a Sct 97A order”. Reference to a “Sct 97A order” occurs in a UK context only. However, following the particularly novel webblocking order granted by the English High Court in *FAPL v BT*, in March 2017, the aforementioned definition needs to be adapted slightly so as to encompass the blocking of illegal streaming servers.

³ In the majority of countries, a webblocking injunction is granted by a court (as is the case in the UK) but, there are exceptions. For instance, in Italy and Portugal,³ the order is granted by an administrative organ. In Italy, the body with the statutory power to order ISPs to block access to copyright infringing material inside or outside Italy is AGCOM. AGCOM stands for Autorità per le Garanzie nelle Comunicazioni. It is, in fact, the regulator and competition authority for the communication industries in Italy. AGCOM’s blocking powers are contained in the Regulation on the Protection of Copyright on Electronic Communications Networks, which came into force on 31 March 2014. In Portugal, the body responsible for notifying local ISPs of the sites to be blocked is the General Inspection of Cultural Activities (IGAC), part of the Ministry of Culture. The blocking process in Portugal is based on a MoU (signed summer 2015) between the Ministry of Culture, ARPITEL (Portuguese Association of Telecommunication Operators), various rightsholders groups, the body responsible for administering Portugal’s .PT domain and representatives from the advertising industry. MAPINET, a local anti-piracy group, also has a role to play in the process as it collates the evidence that is later transmitted to the Ministry of Culture. See: ‘Rapid Pirate Site Blocking Mechanism Introduced By Portugal’ (Torrentfreak, 31 July 2015) <<https://torrentfreak.com/rapid-pirate-site-blocking-mechanism-introduced-by-portugal-150731/>> (accessed 14th June 2017)

⁴ As is posited later in this article, the criterion of effectiveness must involve a measurable and tangible reduction in the amount of online infringement being perpetrated against the claimants’ IPRs. This occurs through a decrease in the number of internet users accessing IP infringing websites and this reduction is facilitated through webblocks.

⁵ As is posited later in this article, the notion of legitimacy (or, acceptability) goes to the general legitimacy or acceptability of webblocking orders. In other words, are webblocks supported by legitimate regulatory purposes and do they pass moral muster?

⁶ To emphasise how important the topic of webblocking is, a large body of academic literature has been written on the subject, much of it relating directly or indirectly to the twin criteria of effectiveness or legitimacy. Some of the more interesting academic articles are (in chronological order): Brian McMahon, ‘Imposing an obligation to monitor on Information Society service providers’ (2011) 17 CTLR 93; Soren Sandfeld Jacobsen & Clement Salung Petersen, ‘Injunctions against mere conduit of information protected by copyright: a Scandinavian perspective’ (2011) 42 IIC 151; Alexandra Giannopoulou, ‘Copyright enforcement measures: the role of ISPs and the respect of the principal of proportionality’ (2012) 3 EJLT Online. <http://ejlt.org/article/view/122/204>; Christina Angelopoulos, ‘Are blocking injunctions against ISPs allowed in Europe? Copyright enforcement in the post-Telekabel EU legal landscape’ (2014) 9 JIPLP 812; Kevin T. O’Sullivan, ‘Enforcing copyright online: internet

As regards the first criterion, effectiveness, the effectiveness of webblocking orders at reducing the incidence of online intellectual property infringement will be assessed by examining a series of leading UK judgments which mark out the UK as a particularly forward-thinking country in this area.⁷ The effectiveness of webblock orders is borne out by a strong trend among countries with mature IP regimes to legislate for, or grant, this type of injunction. But it is not a silver bullet as the effectiveness of webblocking orders can be undermined through *circumvention*, occurring at two distinct levels, the individual infringer⁸ and the website operator. Effectiveness can also be negatively affected by the *territorial nature* of webblocking orders. Pan European blocking orders do not exist, thereby forcing rightsholders to apply for a webblock in each country affected by the infringing activities. However, comparing the elements of effectiveness and ineffectiveness, this analysis will show that the webblocking order is generally effective and, comparatively speaking, more effective than all the other alternative regulatory interventions, currently available to rightsholders.⁹

As regards the second criterion, that of *legitimacy*, this article will assess how legitimate webblocking orders are as a regulatory tool by focusing on legislation (domestic and EU) and the significant CJEU ruling in *Telekabel*.¹⁰ As regards legislation, the analysis breaks down into two distinct components: copyright webblocking orders and, trademark webblocking orders.¹¹ The legitimacy question is less clearcut in the context of UK trademark webblocking

service provider obligations and the European Charter of Human Rights' (2014) 36 EIPR 577; Ruth Hoy, 'Internet blocking injunctions are alive and well in the post *Svensson* world' (2015) 26 Ent LR 44; Richard Arnold, 'Website-blocking Injunctions: the Question of Legislative Basis' (2015) 37 EIPR 623; Althaf Marsoof, 'The Blocking Injunction – A Critical Review of Its Implementation in the United Kingdom Within the Legal Framework of the European Union' (2015) 46 IIC 632; Alpana Roy, 'The Blocking Injunction: A comparative and critical review of the EU, Singaporean and Australian Regimes' (2016) 38 EIPR 92; Paul S. Davies, 'Costs of Blocking Injunctions' (2017) 4 IPQ 330; Alice Blythe, 'Website blocking orders post-*Cartier v B Sky B*: an analysis of the legal basis for these injunctions and the potential scope of this remedy against other tortious acts' (2017) 37 EIPR 770; Eleonora Rosati, 'Intermediary IP injunctions in the EU and UK experiences: when less (harmonisation) is more?' (2017) 12 JILPL 338; and Adebola Adeyemi, 'Liability and exemptions of internet service providers (ISPs): assessing the EU electronic commerce legal regime' (2018) 24 CTLR 6. The survey of the literature would not be complete without reference to the commanding work by Janni Riordan, *The Liability of Internet Intermediaries* (Oxford, 2016). It has a chapter on 'Blocking Injunctions' and a separate chapter on 'Website Blocking in Europe'. In addition, the UK IPO's Report titled "International Comparison of Approaches to Online Copyright Infringement, Final Report (2015/40) proved very helpful in gauging the situation in individual countries.

⁷ Eleonora Rosati, "Intermediary IP injunctions in the EU and UK experiences: when less (harmonization) is more? JIPLP (2017) Vol 12 No 4, 338 at 339 where she describes the UK jurisprudence, based on Sct 97A, CDPA, as "consistent and thoughtful".

⁸ Via encrypted virtual private networks, anonymous proxies and other anonymising tools.

⁹ Taking a pragmatic and logical approach to the complex problem of online IP infringement, the High Court in *Cartier International AG v British Sky Broadcasting Limited*, [2014] EWHC 3354 (Ch) (at [217]) was of the view that currently, there is no real alternative to webblocks in terms of efficacy. This assessment came after the court factored in the state of technological evolution and all the various possible alternatives to the webblocking order. Like many things in life, the webblock is an imperfect solution but still offers acceptable levels of effectiveness so as to be a compelling remedy for the IP rightsholder.

¹⁰ Case C-314/12, *UPC Telekabel Wien v Constantin Film Verleih*, ECLI:EU:C:2014:192.

¹¹ As regards the former, a finding of unquestioned legitimacy is made by the author, as Article 8 (3) of the InfoSoc Directive clearly provides for the possibility of a webblocking injunction throughout all 28 EU Member States. This legitimacy is carried over into the domestic setting (UK) by the relevant secondary legislation that transposes Article 8 (3) into local law (i.e. Regulation 27 of the Copyright and Related Rights Regulations 2003 (SI 2003/2498), which inserted new sections 97A and 191JA into Parts I and II respectively of the CDPA, 1988). The outcome of this transposition – Sct. 97A, CDPA – has been the basis of fifteen written judgments in the area of IP webblocking since 2011 and has been invoked with increasing success by a diversity of rightsholders to produce a rich seam of creative and thought-provoking case-law. The fifteen judgments are as follows:

Twentieth Century Fox Film Corp v British Telecommunications plc [2011] EWHC 1981 (Ch); [2012] Bus LR 1471; *Twentieth Century Fox Film Corp v British Telecommunications plc (No 2)* [2011] EWHC 2714 (Ch); [2012] Bus LR 1525; *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch); [2012] 3 CMLR 14; *Dramatico Entertainment Ltd v British Sky Broadcasting*

orders. The reason for this is a legislative lacuna,¹² which negatively affects the position of UK trade mark holders when it comes to obtaining a webblocking injunction.¹³ Notwithstanding, it shall be demonstrated that, when assessed against the criterion of legitimacy, the webblocking remedy is one which is now regarded as legitimate throughout the entire European Union, following the important CJEU ruling in *Telekabel* in 2014.

2. Testing the Fitness of the Regulatory Environment and Regulatory Interventions Other than the Webblocking Order

The Relationship Between Law and Regulation

As a primary step, it is prudent to try and define regulation and, the relationship between law and regulation. Black defines regulation along the following lines:

*“the sustained and focused attempt to alter the behaviour of others according to standards or goals with the intention of producing broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information gathering and behaviour modification”*¹⁴

As for the relationship between law and regulation, that can be rather unclear. Evidently, the two intersect in society but, frequently, regulation and law are not coterminous as regulation may be a broader or narrower enterprise than law.¹⁵ In the world of online IP infringement, instruments other than legislation are frequently used to either facilitate ISP cooperation in the fight against online IP breaches, or are simply used to reduce the incidence of online infringement. A good example is the code of conduct to which ISPs sign up.¹⁶

Ltd (No 2) [2012] EWHC 1152 (Ch); [2012] 3 CMLR 15; *EMI Records Ltd v British Sky Broadcasting Ltd* [2013] EWHC 379 (Ch); [2013] ECDR 8; *Football Association Premier League Ltd v British Sky Broadcasting Ltd* [2013] EWHC 2058 (Ch); [2013] ECDR 14; *Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd* [2013] EWHC 3479 (Ch); [2014] ECDR 7; *Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd* [2014] EWHC 937 (Ch); *.1967 Limited v British Sky Broadcasting* [2014] EWHC 3444 (Ch); *Twentieth Century Fox Film Corporation v Sky UK Limited* [2015] EWHC 1082 (Ch). *Cartier International AG v British Sky Broadcasting Ltd* [2014] EWHC 3354 (Ch); *Cartier International AG v British Sky Broadcasting* [2016] EWCA Civ 658; *Cartier International Limited v British Telecommunications* [2016] EWHC 339 (Ch); *Football Association Premier League and Others v British Telecommunications and Others* [2017] EWHC 480 (Ch); *Football Association Premier League Ltd v British Telecommunications Plc* [2017] EWHC 1877 (Ch); .¹¹ The outcome of this transposition – Sct. 97A, CDPA, – has been the basis of fifteen written judgments in the area of IP webblocking, since 2011. Moreover, it has been invoked with increasing success by a diversity of rightsholders to produce a rich seam of creative and thought-provoking case-law.

¹² This lacuna occurred through a failure by the UK legislature to transpose the third sentence of Article 11 of the Enforcement Directive into local law. The third sentence of Article 11 ensures that IP rightholders *in general* (not just copyright holders) are in a position to obtain (blocking) injunctions against intermediaries, whose services are used by a third party to infringe an IP right.

¹³ Admittedly, the High Court adroitly filled this lacuna in *Cartier* by a combination of broad statutory interpretation and invocation of the *Marleasing* principle from EU Law. As a consequence of this judicial dexterity, a *form* of legislative legitimacy for trademark webblocking orders now exists in the UK *but*, it is decidedly judge-made in its composition.

¹⁴ Julia Black, “What is Regulatory Innovation?” in Julia Black, Martin Lodge, and Mark Thatcher (eds) *Regulatory Innovation* (Cheltenham: Edward Elgar, 2005) 1, at 11, as cited with approval by Roger Brownsword in, Roger Brownsword, *Rights, Regulation, and the Technological Revolution*, (OUP, 2008), 6.

¹⁵ See generally, the standard functional analysis of ‘law-jobs’ theory in Karl N Llewellyn, ‘The Normative, the Legal, and the Law-Jobs: The Problem of Juristic Method’ (1940) 49 Yale Law Journal 1355

¹⁶ Where voluntary in nature (i.e. conceived by the ISPs themselves), then such code falls outside a legislative initiative.

In the context of webblocking injunctions, (or, on a broader analysis, digital piracy/infringement), the relevant regulatory environment is the internet, a disruptive technology and a prime example of the technological revolution.¹⁷ Within that specific context, *the regulatory intervention* is the webblocking order.

In assessing *the fitness of the regulatory environment* by evaluating webblocking whose effectiveness and legitimacy are being assessed, English case-law will feature prominently in this analysis because the English courts have, through particularly novel and innovative rulings, created the most advanced and sophisticated webblocking regime in the world. Though the webblock has gradually and ineluctably emerged as the primary weapon for copyright holders in many countries in the world, it is beneficial and instructive to first get an overview of alternative regulatory interventions (available to rightsholders) as it will help demonstrate that regulatory intervention is broader than just webblocks and allow the author to highlight any weaknesses in said alternatives.¹⁸

Alternatives to the Webblocking Order

Clearly, through the webblocking mechanism, ISPs are directly engaged in the prevention of online IP infringement. The ISP's role as *private* enforcer of a court or administrative body's webblock order is an important one as, currently, about 25 countries around the world grant webblocks.¹⁹ Admittedly, it is a controversial role as it means that an ISP, for all intents and purposes, a private company, is obligated to do something that must be entirely counter-intuitive: to *block* access to a website!

The webblocking order is not the first anti-infringement process involving ISPs. Over the last two decades, there has been a discernible transfer of responsibility to ISPs in the IP infringement-combatting context.²⁰ This responsibility is to either assist in IP asset protection

¹⁷ Roger Brownsword, *"Rights, Regulation and the Technological Revolution"*, (Oxford, 2008), at p. 4.

¹⁸ The other forms of ISP intervention include graduated response systems (GRS), the notice and takedown system, (which is significantly older and longer established than the webblock order, having been legislatively provided for by the 2000 E-Commerce Directive), ISP codes of practice and lastly, the Norwich Pharmacal Order (NPO), which not so long ago, was the principal 'route' for rightsholders to try to obtain a remedy against online as infringers.

¹⁹ In her article "Next chapter in ISP's Blocking Battle: Dutch Supreme Court refers questions about indirect infringement by operators of the Pirate Bay to the CJEU", Van den Heuvel states that 13 European countries have granted webblocks up to now, with Italy and the UK being the most prolific granters (in that order). *European Intellectual Property Review* (2016) 38 (9), 577 at 580. To this list of 13, Sweden should be added, as it granted its first webblock order in 2017, subsequent to Van den Heuvel's article.

²⁰ In this regard, see the thought-provoking views of Natasha Tusikov in *Chokepoints – Global Private Regulation on the Internet* (University of California Press (2017)). In her work (at p. 49), Tusikov sees a gradual evolution towards 'internet intermediaries' becoming 'de facto regulators', with that evolution possibly starting as early as 1994 when, then Vice President, Al Gore, outlined a shift from a "traditional adversarial" regulatory relationship between business and government to one based on "consensus" in relation to the internet. Tusikov observes that governments may work indirectly with intermediaries by setting regulatory targets or prescribing specific regulatory frameworks or enforcement practices that intermediaries must adopt. As with many informal agreements, governments may prefer to direct intermediaries to act in the absence of specific legislation or court orders. Another interesting observation made by Tusikov (at pp 50 & 51) is that increasingly, rightsholders are demanding that intermediaries take on expanded regulatory roles. The reasons for this are as follows: intermediaries generally have valuable technical skills, they have access to specialised information or systems and, they possess the capacity to monitor or control flows of information across their platforms. In addition, ISPs may be more responsive and adaptive to changes in technology or circumstances than regulation through legislation or, international law or agreements. On a practical note, it could be argued that many internet intermediaries

or in the prevention of IP infringement. Examples of alternative regulatory interventions (i.e. apart from webblocking orders) in which ISPs play an active role in IP infringement prevention include: the graduated response systems (GRS); notice and takedown regimes; codes of conduct, and, Norwich Pharmacal Orders (NPO), all of which shall be discussed below.

The Graduated Response System ('GSR')

The GRS is often viewed as a soft mechanism for digital copyright enforcement that requires ISPs, rightsholders and an industry regulator to operate a scheme by which primary infringers can be identified, educated and penalised.²¹ These GRSs sometimes take the form of a statutory 'three strikes' regime, such as was provided in the Digital Economy Act (2010) and represent an attempt to alter the legal and procedural rules of the game, by establishing a non-monetary enforcement scheme.²² The element common to all GRSs is that ISPs are required to take some action against subscribers accused of infringing copyright.²³

Two of the first countries to implement a form of GRS were France and New Zealand. France's GRS is built around an independent public agency dedicated to the prevention of online copyright infringement.²⁴ The agency, the *Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet* (HADOPI), administers the three stage GRS against individuals suspected of acts of infringement committed on P2P networks. HADOPI is, in effect, an intermediary between internet users, right holders, ISPs and the French criminal courts. While the end game of the three stage process is a series of punitive sanctions (fines and technical measures to restrict the performance of internet access), the main purpose of the three stage notification process is to change consumer behaviour about copyright.²⁵ However, France's so-called HADOPI laws proved controversial almost from day one and they became decidedly mired in controversy in 2013 when the French Constitutional Council

are already *de facto* regulators of online life by virtue of the rules they set through their terms of use agreements. After all, these rules, for all intents and purposes, decide what information people can access, use and share online.

²¹ See generally, Yana Breindl and Francois Briatte, 'Digital Network Repertoires and Contentious Politics of Digital Copyright in France and the European Union' (Paper presented at the Oxford Internet Institute conference, Oxford, 16 September 2010), 6.

²² Jaani Riordan, *The Liability of Internet Intermediaries*, Oxford, 2016, 149.

²³ Nicolas Suzor and Brian Fitzgerald, 'The Legitimacy of Graduated Response Schemes in Copyright Law', (2011) 34 *University of New South Wales Law Journal* 1,1.

²⁴ For a good account of France's GRS, see the UK IPO Report titled "International Comparison of Approaches to Online Copyright Infringement, Final Report. (2015/40), pp 44-48.

²⁵ The so-called HADOPI laws were controversial from the very start and experienced a major setback in July 2013 when the country's Constitutional Council ruled that portion of the much criticised law was unconstitutional. A subsequent decree by the Council stated that the government could no longer suspend users' internet access for copyright violation. Instead, only fines would be imposed, starting at a meagre €60 and increasing, based on the number of infractions. This move reflected a change in the government's policy of pursuing individual infringers to one of fighting "commercial piracy" or "sites that profit from pirated content". HADOPI was also criticised for being very expensive to run with non commensurate returns in terms of illegal file-sharing stopped. See: France drops controversial 'Hadopi law' after spending millions, 9th July 2013, (<https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy>), accessed 29th January 2018.; France's 'three strikes' anti-piracy law shot down - Fines only for internet copyright infringers from now on, by Neil McAllister, 9th July 2013 (https://www.theregister.co.uk/2013/07/09/france_three_strikes_piracy_law_shot_down/)(accessed on 29th January 2018).

held internet access to be a basic human right²⁶. This decision fundamentally impugned the French GRS measure of disconnecting the internet services of the most stubborn IP infringers. Like France, the New Zealand system (a ‘three strikes’ law) also proved controversial. Its system came into force in September 2011²⁷ and is operated in the first instance by the New Zealand Copyright Tribunal but with a right of appeal to the High Court.²⁸ While a webblock can certainly cause irritation for some internet users, it is nothing compared with the drastic step of internet disconnection. Given the highly targeted and specific nature of a webblocking injunction, it is, in reality, a much more subtle and precise tool for tackling online IP infringement than the more draconian (and potentially unconstitutional) measure of internet disconnection.

Notice and Takedown

In the EU, ISPs and webhosts play an important role in the removal of copyright infringing material from their network/platform in the framework of the notice and takedown system. This system, contained in the (2000) E-Commerce Directive²⁹ provides an exemption from liability to ISPs/webhosts which act expeditiously to remove or disable access to infringing material, once they become aware of its presence on their communication network/electronic platform. A similar system exists in the U.S. under the Digital Millennium Copyright Act, 1998 (DMCA)³⁰ where the safe harbour is only available to an ISP that “acts expeditiously to remove or disable access to the (infringing) material”.³¹

26 *France drops controversial ‘Hadopi law’ after spending millions*, by Siraj Datto, 9th July, 2013, (<https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy>), (accessed 10th February, 2018)

27 By virtue of the Copyright (Infringing File Sharing) Amendment Act 2011.

28 See Graeme B. Dinwoodie (Editor), *Secondary Liability of Internet Service Providers*, (Ius Comparatum – Global Studies in Comparative Law), Springer (2017), at 49; <https://www.lawsociety.org.nz/lawtalk/lawtalk-archives/issue-832/infringing-file-sharing-two-years-on> (Article titled “Infringing File Sharing Two Years On”, by Kate Duckworth, 22 November 2013 (accessed 28th January 2018); In New Zealand, the “three strikes” law proved controversial because it makes account holders responsible for the copyright infringement regardless of who uploaded/downloaded the material. Potentially, therefore, flatmates, parents, cafés and employers could be liable for illegal file sharing carried out by third parties on their internet accounts.

29 See, Directive 2000/31/EC of 8th June, 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, (17th July, 2000), p. 1-16). Article 14 (on Hosting). Article 14 (1) provides as follows: 1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or, (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

30 See Sct 512 (c) of that Act.

31 E-Commerce companies were quick to adopt the idea of notice and takedown. In the same year as the coming into force of the DMCA, eBay created a notice and takedown programme called VeRO, the Verified Rights Owner Program. In this program, rightsholders submit complaints to eBay regarding sales listings for counterfeit goods and eBay removes the listings. See Natasha Tusikov, *Chokepoints – Global Private Regulation on the Internet*, (California Press, 2017) at 55. Tusikov makes the astute observation that there is no judicial or government oversight of either the formal (E-Commerce Directive/DMCA) or informal (eBay) notice and takedown programs. These programs have been the subject of criticism from the likes of the digital rights group, Electronic Frontier Foundation, who point out that these programs are based solely on accusations, not proof, of infringement. All that is required from rightsholders is a declaration in good faith that they believe their IPRs are being violated. Informal anti-counterfeiting agreements, such as eBay’s, are intended to make enforcement more streamlined and rapid, and in fact intermediaries are processing an increasing number of cases of infringement, based only on rightsholders’ complaints. The Chinese notice and takedown regime resembles the E-Commerce and DMCA. It is based on revisions made to Article 36 of the country’s Tort Liability Law, which sets out the conditions under which internet intermediaries are liable for the infringement of IPRs. Article 36 allows rightsholders to require intermediaries to remove, block or disable access to infringing material. As regards China, see

The virtually identical wording of the EU provision and the US provision shows that the EU legislators drew significant inspiration from their counterparts in the U.S. Interestingly, in Canada, ISPs participate in a *statutory notice and notice system*, rather than a *notice and takedown system*. The Canadian system has been operational since January, 2015 and is contained in the country's 2012 Copyright Modernization Act. Under the notice and notice system, the ISP does not take down the infringing material. Rather, it forwards the copyright holder's notice of infringement to the uploader "as soon as feasible", the overall aim of the system being to discourage further infringement. The notice of infringement contains information that will assist the uploader understand the details of the allegation, including the date and time of the alleged conduct.

When comparing the webblocking regime with the notice and takedown system, it has to be borne in mind that the former has important *inbuilt safeguards* that are aimed at protecting the freedom of expression and preventing abuse on the part of rightsholders. One of the principal safeguards is that the decision to block a website is taken by a court of law, implying the presence of transparency, accountability and balance, key elements of any dispute resolution system.³² In stark contrast, the notice and takedown approach *lacks* these key elements, as it involves a private sector company making a judgement on whether potentially infringing material needs to be removed from its communication network. A further *weakness* of the notice and takedown system is that ISPs frequently take down material expeditiously but without a careful consideration of its illegality (or otherwise). This cautious approach by ISPs is influenced by their own interests and a desire to avoid potential liability. But, this approach may result in entirely legitimate material being removed from their networks, in effect, an erroneous decision, potentially affecting an innocent third party's commercial interests or IPRs. Moreover, such an unnecessary takedown also deprives internet users of access to (legitimate) information.³³ As the notice and notice system has even less teeth than the notice and takedown system (being designed primarily to discourage online infringement rather than to actually tackle infringement), the case for a webblocking injunction over a notice and notice system is unanswerable.

Codes of Practice

Attempts have been made in certain countries to get ISPs to sign up to Codes of Conduct to assist in the fight against online copyright infringement. Good examples include Denmark

Natasha Tusikov, *Chokepoints – Global Private Regulation on the Internet*, (University of California Press, 2017), at 161. In the same work (at pp 181-183), Tusikov describes Taobao's notice and takedown system.

³² Althaf Marsoof, The blocking injunction - a critical review of its implementation in the United Kingdom in the context of the European Union, IIC 2015, 46(6), 632 at 649.

³³ Althaf Marsoof, The blocking injunction - a critical review of its implementation in the United Kingdom in the context of the European Union, IIC 2015, 46(6), 632 at 633. However, not all academic commentators are so negatively disposed towards the notice and takedown procedure. For instance, Riordan sets out three advantages of notice and takedown in his work, *The Liability of Internet Intermediaries* (Oxford, 2016), at 462 and 463. They are: Removal of material is both outright and universal. Once data have been removed, they are inaccessible regardless of which ISP is used (Blocking is specific to the targeted service, meaning that separate blocks must be implemented by a different group of ISPs in each jurisdiction); 2. Removal destroys the infringing material (in contrast, blocking allows the infringing material to remain. Consequently, the material can still be accessed by individuals accessing the infringing websites from countries in which no webblocks were granted. This goes to the territorial nature of the webblock); 3. Subject to the risk of mirror websites or repeat postings, removal is absolute (blocking is imperfect and can be circumvented by various technical means).

and the UK. In 2014, the Telecommunications Industry Association (Teleindustrien) in Denmark signed a code of conduct defining the conditions of voluntary website blocking by Danish ISPs. Under the code, ISPs commit to implement webblocks within 7 days of the court order/order granted by the administrative authority. The aim of the Danish code is to set up a one stop shop for website blockings at DNS level. It also aims to ensure that the webblock can be expanded to other websites, where an infringing website changes its domain name.³⁴ The Danish code initiated a paradigm shift about the enforcement and regulation of consumer behavior on the internet. Under the code, Danish ISPs are required to inform internet users about webblocks implemented by them. ISPs achieve this by attaching a communication to the blocked website, explaining why the website is blocked and, importantly, guiding the internet users to alternative *legal* sources of the copyrighted material. During the first twelve months of the code's existence, hundreds of thousands of Danish consumers visited the alternative *legal* sources.³⁵

The UK introduced a Code in 2010 but it never came into effect. The Digital Economy Act (2010) imposed a duty on OFCOM, the communications regulator, to set out a code of conduct for ISPs that dealt with online I.P. infringement.³⁶ OFCOM set out its draft code in May 2010 for consultation³⁷ but the consultation was delayed for two years. This was due to the ISPs seeking a judicial review of the legislation and the statutory instrument permitting costs to be imposed on the ISPs.³⁸ Ultimately, in March 2012, the Court of Appeal held in favour of the ISPs.³⁹ This caused OFCOM to issue a revised code, with a notice of its intention to seek its statutory implementation.⁴⁰ While the main elements of the March 2012 code were substantially similar to the May 2010 version, the 2012 code never came into force either. It seems a combination of UK Treasury constitutional concerns and leaked Government reports expressing anxieties about possible subsequent litigation if the code came into force⁴¹ sounded the death knell for the revised code. Instead, an industry solution,

³⁴ Maria Fredenslund (RettighedsAlliancen), "Denmark: Code of Conduct on Website Blocking" <http://copyrightblog.kluweriplaw.com/2014/10/24/denmark-code-of-conduct-on-website-blocking/>, 24th October, 2014 (accessed on 4th February, 2018).

³⁵ Maria Fredenslund (RettighedsAlliancen), "Denmark: Code of Conduct on Website Blocking" <http://copyrightblog.kluweriplaw.com/2014/10/24/denmark-code-of-conduct-on-website-blocking/>, 24th October, 2014 (accessed on 12th February, 2018).

³⁶ Digital Economy Act 2010 s.6 see also Communications Act 2003 s.124D(1).

³⁷ OFCOM, 'Online Infringement of Copyright and the Digital Economy Act 2010: Draft Initial Obligations Code (28th May 2010)' <https://www.ofcom.org.uk/__data/assets/pdf_file/0022/59071/condoc.pdf>

³⁸ *R. (on the application of British Telecommunications Plc) v Secretary of State for Business, Innovation and Skills* [2011] EWHC 1021; [2011] 3 CMLR 5.

³⁹ *R. (on the application of British Telecommunications Plc) v Secretary of State for Business, Innovation and Skills* [2012] EWCA Civ 232; [2012] 2 CMLR 23.

⁴⁰ OFCOM, 'Online Infringement of Copyright and the Digital Economy Act 2010: Notice of Ofcom's proposal to make by order a code for regulating initial obligations' (26th June 2012) <https://www.ofcom.org.uk/__data/assets/pdf_file/0032/45986/notice.pdf>

⁴¹ <https://www.out-law.com/en/articles/2013/june/ofcom-anti-piracy-code-delayed-until-2015/>

the Creative Content UK initiative (CCUK), was implemented in July, 2014.⁴² Arguably, however, an initiative such as the CCUK is more *persuasive* in nature and lacks the ‘bite’ and tangible impact on online IP infringement that a webblock possesses.⁴³ ¹

Norwich Pharmacal Orders

Despite their decline in popularity in terms of IP infringement prevention, NPOs have also played an important role in the background narrative. Like the majority of webblocking orders, NPOs are court orders granted against ISPs. However, they have a *different objective* to webblocking orders. Under a NPO, an ISP is required to disclose certain information to the (rightsholder) applicant. Normally, the private details of suspected copyright infringers are disclosed under NPOs. Armed with this important information, the prejudiced rightsholder would then decide whether or not to sue the suspected IP infringer.

Prior to the emergence of the webblocking order in the UK in 2011,⁴⁴ the equitable remedy of the NPO was relied on quite a bit by rightsholders. The granting of a NPO in no way alleviates an infringement scenario, it just provides the applicant rightsholder with possible evidence. Unsurprisingly, therefore, the webblocking order, has, for the most part, supplanted the NPO.⁴⁵

3.The criterion of effectiveness

What does “effective” mean in a webblocking context? A measurable and tangible reduction in the amount of online infringement being perpetrated against the claimants’ IPRs is probably the simple answer. But, this can only occur if there is a decrease in the number of internet users accessing IP infringing websites. Developing the definition of ‘effectiveness’ further and, viewing IP protection from a macro perspective, one would have to argue that true effectiveness only really occurs if those migrating from the blocked websites (or servers) *change their behaviour* and attitude and stop (or significantly reduce) their access to infringing websites altogether. If this happens, then an important attitudinal change will have occurred, something that may well presage a time in the future when webblocks are no

⁴² This is a product of the Voluntary Copyright Alert Programme, which facilitates discussions between a number of key stakeholders. The CCUK consists of two elements, a major multi-media public education campaign and a programme of email alerts sent by ISPs to residential broadband subscribers when their account is used to infringe copyright. Like the three stage GRS in France, mentioned above, the UK initiative has a strong educational component, whereby internet users are informed about the wide range of legal sources of content available to them. In addition, the initiative promotes awareness of the value and benefits of creative content and the copyright which underpins it.

⁴³ <http://www.creativecontentuk.org/> (accessed 10th February, 2018); <https://www.gov.uk/government/news/new-education-programme-launched-to-combat-online-piracy> (accessed 10th February, 2018); and <https://www.lexology.com/library/detail.aspx?g=b4448ea9-d346-4830-bac3-09ad0c7dd899> (accessed 10th February,

⁴⁴ The seminal case being: *Twentieth Century Fox v British Telecommunications Plc* [2011] EWHC 1981 (colloquially known as the *Newzbin2* case).

⁴⁵ Pointedly, in *Cartier International Limited v British Telecommunications 2016* [2016] EWHC 339 (Ch). Hacon J, referring to Arnold J’s statement in *Cartier*, stated (at [15]) that the analogy between the blocking order and a NPO should ‘not be pushed too far’. It was Arnold J’s way of demarcating the webblocking regime from the NPO regime and possibly also indicating a supplanting of the latter by the former. While the NPO facilitates proceedings against individual IP infringers, the webblocking injunction circumvents potentially cumbersome, expensive and protracted litigation against individual infringers. Instead, it prevents potential infringers accessing websites that facilitate/promote IP infringement. Preventative rather than reactive in nature, the webblocking injunction attempts to keep Pandora in her box! In many ways, therefore, Section 97A litigation is, strategic litigation. In opting for a webblocking injunction, the rightsholder will, in all likelihood, avoid more extensive and costly litigation in the future.

longer needed. In this section of the article, the author will examine the effectiveness of webblocking injunctions from two distinct perspectives: the judicial view of their effectiveness and the academic view.

The Judicial View of Effectiveness

Given the cost and inconvenience meted out to defendant ISPs in the shape of a webblock order, one might argue that the diminution in infringing activity, post-injunction, would need to be fairly substantial. But, the English courts go further, adopting a more hard-headed, realistic and pragmatic approach, best exemplified by the English High Court's assessment of the efficacy of webblocks in *Cartier International AG v British Sky Broadcasting*.⁴⁶

There, the High Court acknowledged that experienced and determined users would continue to circumvent blocking measures but that fact should not negate the usefulness of the webblocking order.⁴⁷ Arnold J regarded Sct 97A orders as "reasonably effective" in reducing the use of infringing websites in the UK and generative of a "worthwhile outcome".⁴⁸ While this assessment may sound like lukewarm praise, it has to be seen in the light of a particularly challenging digital environment for rightsholders where even small victories can, in reality, be considered as large victories!⁴⁹

The effectiveness of a webblocking order is often best measured (and demonstrated) through the prism of internet traffic data. New trends or sudden changes in internet traffic often

⁴⁶ *Cartier International AG v British Sky Broadcasting Limited*, [2014] EWHC 3354 (Ch), at [218] to [237] In *Cartier*, the claimants owned a large number of UK registered trade marks, including CARTIER, MONTBLANC, IWC and other brands. They sought orders requiring the ISPs to block access to six websites that infringed their Trade Marks by advertising and selling counterfeit goods. The target websites each targeted UK customers offering for sale replicas of products bearing one of the Trade Marks. Mr Justice Arnold granted the orders, finding the likely costs burden on the ISPs was justified and the orders were proportionate. To safeguard against abuse, the ISPs and operators can apply to the Court to discharge/vary the orders following a change in circumstances, and the orders will cease to have effect after a defined period (provisionally set at two years) unless either the ISPs consent or the Court orders that they should be continued. *Cartier's* significance arises from the fact that it was the first ever webblock granted in the UK in relation to online trade mark infringement.

⁴⁷ *Cartier International AG v British Sky Broadcasting Limited*, [2014] EWHC 3354 (Ch), at [236].

⁴⁸ *Cartier International AG v British Sky Broadcasting Limited*, [2014] EWHC 3354 (Ch), at [236].

⁴⁹ In a case such as *Cartier*, where technology and more appositely, the internet loomed large on both sides of the dispute, it is unsurprising that the claimant trademark holders' case was built on expert evidence, almost all of it digital in nature, and submitted to court by way of two expert reports. Equally unsurprising is the fact that companies like Alexa and, Incopro Ltd featured so prominently in the *Cartier* judgment as both are inextricably linked with the provision of technical services to assist in combating online intellectual property infringement. Interestingly, the expert witness' analysis of the estimated usage data for proxies demonstrated that there was no evidence of any major migration of UK users of the targeted websites to proxies. Further, using Google Trends, the expert witness observed no major spike in internet searches for search terms relating to VPNs and Tor on or subsequent to the date of the actual webblock. These findings were already highly positive from an infringement prevention standpoint. Alexa Internet, Inc is an American company that provides commercial web traffic data and analytics. It is a wholly owned subsidiary of Amazon.com. INCOPRO is a UK company that delivers innovative technology-based solutions to businesses facing IP infringement challenges online. One of its key services is the provision of global anti-piracy intelligence. The company's IDENTIFY system was created for content owners to provide a comprehensive global overview of online infringement of protected content. According to the company's website, IDENTIFY is currently tracking over 17,000 sites that are engaged in facilitating copyright infringement and is continuously discovering new sites. (website accessed 15th January, 2018). A virtual private network (VPN) gives you online privacy and anonymity by creating a private network from a public Internet connection. VPNs mask your Internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections, guaranteed to provide greater privacy than even a secured Wi-Fi hotspot. Similarly, the Tor browser is a tool designed to make the user anonymous online, without using VPN technology or encrypting data. The name Tor is an acronym for 'The Onion Router,' which is a specialized browser that sends the user's data through several anonymous servers. In doing so, it becomes considerably more difficult to identify what the user is doing online.

present a clear picture about internet users' habits and decisions. Unsurprisingly, therefore, internet traffic data often constitutes the 'backbone' of expert evidence in a webblocking case.⁵⁰

But, in an even more illuminating statement on webblocking effectiveness, Arnold J, alluding to the fact that *Cartier* was in fact an online *trade mark* case (as opposed to an online copyright case), offered the interesting view that a webblock in *Cartier* could in fact be more effective than a webblock in the copyright infringement cases because internet users had little brand loyalty to the target websites in *Cartier*, whereas a website like the Pirate Bay website (involving copyright infringement) does have quite a loyal user base. In other words, fickle internet users are much more likely to be deterred by a webblock, than would stalwart users who have strong allegiance to a specific website such as Pirate Bay.

Further judicial insight on the theme of the effectiveness of webblocking injunctions was provided by the 2017 ruling in *Football Association Premier League Limited v British Telecommunications Ltd* (FAPL v BT),⁵¹ this time in a new context. The judgment is unique as it concerns illegal streaming servers rather than "run of the mill" illegal websites. Given the distinct nature of the case, it was always going to be a type of 'litmus test' for the effectiveness of webblocking in a streaming server context, but also serves as a 'rolling commentary' on how webblocking was performing generally and, specifically, in the light of technological advances. The outcome of FAPL was clearcut: it *pointed resolutely towards increased effectiveness*.

Conspicuously, it was also very clear in *FAPL* that Mr Justice Arnold's views on the effectiveness of webblocks had grown stronger over the intervening three years. This was evident from the learned judge agreeing with the claimant's contention that a webblocking order would be effective, dissuasive and substantially reduce infringements of its copyrights. Arnold J offered *five factors* to support his viewpoint. Chief among the five reasons was his

⁵⁰ In *Cartier*, the analyses carried out by claimants' expert witness showed a consistent pattern. In each case, the UK data shows a marked and sustained drop in traffic to the targeted websites after the date on which the blocking order was implemented. By comparison, the global data excluding the UK did not show anything like this. The striking contrast between UK and global traffic is made evident through the expert witness's analysis of the top 100 video streaming link websites (i.e. websites which infringe film and television copyrights). This analysis showed that the UK experienced a significant decrease in traffic to blocked websites (-71.2%), whereas the rest of the world experienced an increase in traffic to those websites (27.8%) (at para [228] of the judgment). This would all suggest that many UK users who had been blocked from accessing infringing websites by Sct 97A orders did not circumvent the blocks but started using different websites instead. One can only hope that these alternative websites were legitimate, copyright compliant websites but Arnold J was content to give these migrating internet users the benefit of the doubt when he declared that the foregoing statistics suggested that "the section 97A orders have resulted in a decrease in the overall level of infringement in this sector in the UK". (at para [228] of the judgment).

⁵¹ [2017] EWHC 480 (Ch), In *FAPL v BT*, the claimant sought a blocking order under Sct 97A, CDPA, but in relation to illegal streaming servers rather than infringing websites. The focus of the Order on streaming servers (rather than websites) reflects the fact that consumers are increasingly using set-top boxes, media players and devices that use software (such as Kodi) to connect directly to infringing streams. The High Court granted the order sought, an order that was unique for the following reasons: 1. It was directed at "target servers" rather than target websites; 2. A prescribed notification procedure allows the ISPs to access the list of IP addresses to be blocked as close to *simultaneously as is reasonably practicable*; 3 The list of target servers is "re-set" each match week during the Premier League season, to ensure that servers which are no longer sources of infringing footage do not continue to be blocked; 4. The Order has effect only for a short period (until 22 May 2017 when the 2016/17 Premier League season ends); and, 5. The Order requires a notice to be sent to each hosting provider each week when one of its IP addresses is subject to blocking.

reference to “past experience” and how it suggests that blocking causes a material reduction in the number of UK users who access blocked websites. In that regard, he referred to all of the expert evidence reviewed by him in *Cartier* (discussed above) and opined that blocking illegal streaming servers (as opposed to illegal websites) would have a similar effect for UK internet users.⁵²

Markedly, the Court highlighted the importance of technological improvements as a key contributor to *enhanced effectiveness*, observing that when granting a novel “live” blocking order in the case, that such an order was made possible thanks to two important technological advances,⁵³ , which also allow the nature and character of the webblocking order to evolve in tandem with technological improvements. Enticingly, the judgment also hints at possible further technological advances on the horizon which should render the webblocking processes more effective as they will become more responsive to changes in IP addresses.⁵⁴

How Effectiveness Is Viewed in the Academic World

When it comes to the academic literature, there seems to be rather mixed feelings about the effectiveness of the webblock. Meale is most positively disposed to the webblock, describing the blocking jurisdiction in the UK as “a real success for rightholders”. Viewing the webblock as a “very useful weapon” (for now), he does concede however that the law always lags behind technology and that, over time, webblocks may lose their effectiveness.⁵⁵ Rosati, referring specifically to the UK situation, describes the webblock as “a successful remedy in the hands of rightsholders”,⁵⁶ Marsoof is slightly more circumspect. He views the new

⁵² The four other factors were as follows: 1. Recent academic research from the Carnegie Mellon University (USA), focusing on UK webblocks (from 2014), which showed that those webblocks significantly reduced access to copyright infringing websites, resulting in a notable decline in overall piracy rates and increased consumption of legal content by respectable percentages; 2. Blocking access to streaming servers is likely to be more effective than blocking websites which embed or link to streams from such servers both because streaming servers are the crucial link and because multiple websites typically embed or link to each server stream; 3. Monitoring and blocking techniques employed by FAPL and the Defendants respectively have improved considerably since earlier blocking orders were made. Improved automation and the investment of manual resources to carry out blocking at the relevant times have contributed to the general improvements. Collectively, these improvements make it feasible to identify and block target servers much more rapidly than before, leading to the prevention of an even greater proportion of potential infringements; 4. There is reason to hope that blocking access to the Target Servers will help to educate UK consumers that accessing infringing streams is not a lawful or reliable way to access Premier League content.

⁵³ They are: new video monitoring technologies (used by the claimant, FAPL) and, advances in certain of the Defendants’ blocking systems permit identification of infringing streams with a very high level of accuracy and, blocking/unblocking of IP addresses during the course of Premier League matches, respectively. Naturally, these two advances will further augment the level of *effectiveness* of webblocking generally.

⁵⁴ *Football Association Premier League Limited v British Telecommunications PLC*, [2017] EWHC 480 (Ch), at [24]. The possible technological advance is the automation or, possible manual supervision of the Defendants’ blocking system. This would enable the blocking to be more responsive to changes in the IP addresses being used by the operators of the illegal streaming services at the times when blocking is most needed to protect the IPRs in question. The advance would also mean that blocking need not occur outside of match times.

⁵⁵ Darren Meale, *Cartier: blocking injunctions given a resounding thumbs up by Court of Appeal*, JIPLP (2016) Vol. 11, No. 11, 818 at 821.

⁵⁶ Eleonora Rosati, *Intermediary IP injunctions in the EU and UK experiences: When less harmonisation is more?*, JIPLP (2017), Vol 12, No 4, 338 at 349.

approach in Europe (to webblocks) as gaining in popularity and describes the blocking injunction as “a pragmatic solution”.⁵⁷ Riordan seems non-committal on the specific matter of effectiveness.⁵⁸

However, research undertaken in recent years in the U.S.⁵⁹ provides strong empirical evidence on the effectiveness of webblocks. Acknowledging that website blocking has become a “primary tool” in the efforts to mitigate the impact of online piracy on media sales, research conducted by Danaher, Smith and Telang analysed the effect on consumer behaviour of UK court orders blocking 53 different piracy websites in November 2014. The report’s findings are compelling. In short, the research found that the 53 blocked websites caused a 90% drop in visits to the blocked sites, and led to a 22% decrease in total piracy; a 6% increase in visits to paid legal streaming sites like Netflix, and a 10% increase in videos viewed on legal ad-supported streaming sites like BBC and Channel 5. Cumulatively, this evidence suggests that blocking large numbers of websites *can alter consumer behaviour*, and can mitigate the possibility of a long-term return to the prior status quo. The two headline statistics i.e. the 90% drop in visits to blocked websites and the 22% decrease in total piracy are very significant, particularly, the former.

Effectiveness Eroded?

However, despite strong evidence from the courts (UK and foreign) that webblocking orders are effective and currently the best remedy against online IP infringements, the remedy also has vulnerabilities. There are two main threads of criticism, they are: the risk of circumvention and, the need for multiplicity of proceedings.⁶⁰

Risk of Circumvention

With all technological solutions, the risk of circumvention is ever present.⁶¹ Technological ‘props’ only remain efficacious so long as the majority of internet users fail to circumvent

⁵⁷ Ahthaf Marsoof, *The Blocking Injunction – A Critical Review of Its Implementation in the United Kingdom Within the Legal Framework of the European Union*, IIC (2015) 46: 632 at 633.

⁵⁸ Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford, 2016).

⁵⁹ In fact, this U.S. research was one of the five factors set out by Arnold J in *FAPL v BT* for evidencing growing effectiveness of webblocks. The title of the 2016 report is: “*Website Blocking Revisited : The Effect of the UK November 2014 Blocks on Consumer Behaviour*” It was co-authored by Brett Danaher, Michael D. Smith and Rahul Telang of the School of Information Systems and Management, Heinz College, Carnegie Mellon University (USA) and was carried out as part of the Initiative for Digital Entertainment Analytics (IDEA).

⁶⁰ See: Dr Alpana Roy and Althaf Marsoof, “The blocking injunction: a comparative and critical review of the EU, Singaporean and Australian regimes” *European Intellectual Property Review*, (2016), 38 (2).

⁶¹ This fact is readily acknowledged by Arnold J. in *Cartier v British Sky Broadcasting*, [2014] EWHC 3354 (Ch), at [26], [27] and [236]. At [26], Arnold J states that the 4 main blocking techniques referred to in his judgment (at [25]) “can readily be circumvented by users who have a little technical knowledge and the desire to do so”. The 4 techniques are: DNS name blocking; 2. IP address blocking user routers; 3. DPI-based URL blocks and, 4. Two Stage systems. Rather ominously, Mr Justice Arnold states that DNS name blocking is the easiest to circumvent but that the other techniques can also be circumvented without difficulty. He also lists the two principal circumvention methods: proxy servers and virtual private networks. At [27], he refers to circumvention methods used by the operators of illegal websites. They are changing IP addresses and URLs.

them, and technologically savvy internet users fail to create or master a circumventory route. But, technology, like a double-edged sword, carries risks for IP rightsholders too. While sophisticated technology is used by IP rightsholders to detect online infringements, and by ISPs to implement the webblocks, technology can also be deployed by individual infringers to both infringe digital IP and to circumvent webblocks. For example, circumvention of webblocks can be achieved through the use of encrypted virtual private networks, anonymous proxies, and other anonymising tools.⁶²

Besides the aforementioned individual infringer instance, there also exists the intractable instance of circumvention by the operators of the blocked websites themselves. Arguably, this is considerably more worrying because it renders the core problem (of the infringing website) less remediable. This type of circumvention occurs through the changing of the IP addresses or uniform resource locators (URLs) of the relevant website.⁶³

While individual user based circumvention will always be difficult to stamp out, the UK approach to tackling circumvention on the parts of the owners/operators of the infringing website is arguably both innovative and revolutionary. This approach involves the use of the *notice and block procedure*.⁶⁴ In the UK, rightsholders are permitted to directly notify ISPs (subsequent to the grant of a webblocking order) where an online location changes its IP or URL. This is permitted *without* a separate application to court. In essence, this means that the ISPs update their blocking databases with the assistance of the rightsholders, but, the overall net effect is *circumvention prevention* and, consequently, *greater effectiveness*.

So well established has the notice and block ‘facility’ become in the UK that Arnold J refers to it as “standard practice” in his 2017 judgment in *FAPL v BT*.⁶⁵ And, seeing no good reason to diverge from this effective practice, Arnold J, in his Order in that particular case, provides for the list of target servers to be “re-set” each match week during the Premier League. This

⁶² Althaf Marsoof, “The Blocking Injunction – A Critical Review of Its Implementation in the United Kingdom Within the Legal Framework of the European Union”, IIC (2015) 46: 632 at 653 and, OFCOM Report titled “Site Blocking to Reduce Online Copyright Infringement – A Review of Sections 17 and 18 of the Digital Economy Act” (May 2010), at pp 8, 33 and 38 (accessed 20th January, 2018). ”

⁶³ In simple terms, a change in IP address is akin to a change of location, in other words, the content is moved from the blocked location to a new location. On the other hand, a change in URL is akin to change in the route to the online location. See: Dr Alpana Roy and Althaf Marsoof, “The blocking injunction: a comparative and critical review of the EU, Singaporean and Australian regimes” European Intellectual Property Review, (2016), 38 (2), 92 at 99.

⁶⁴ The phrase “notice and block” has been coined by Marsoof to describe this novel feature of the UK webblocking regime. It should be noted however that this innovative and supremely pragmatic approach is a court inspired *modus* as the two relevant legislative provisions in the UK, namely sct 97A and sct 191 JA of the CDPA, 1988 do not contemplate such a practice. Nor do the two relevant EU Directives. As to the phrase “notice and block”, see Althaf Marsoof, “Blocking injunctions protect trade mark rights on the internet” (2015) 10 (3) Journal of Intellectual Property Law & Practice 158, 163. Generally, see, Alpana Roy and Althaf Marsoof, “The blocking injunction: a comparative and critical review of the EU, Singaporean and Australian regimes” European Intellectual Property Review, (2016), 38 (2), 92 at 99. Interestingly, despite the evident usefulness of the UK notice and block facility from an effectiveness perspective, neither Singapore nor Australia (both acknowledged mature IP Law systems) has accommodated IP rightsholders along similar lines. The author posits that this proves two things, firstly, that the UK courts have, through their rulings, helped ‘craft’ one of the most advanced, innovative and flexible webblocking regimes in the world. Secondly, so long as Singapore and Australia ignore the clear benefits of the notice and block facility, the level of effectiveness in their blocking systems will be sub-optimal. As a point of mitigation, however, those countries’ only adopted blocking legislation relatively recently, Singapore in 2014 and Australia in 2015.

⁶⁵ *Football Association Premier League v British Telecommunications PLC*, [2017] EWHC 480 (Ch), at [25].

flexibility allows for the inclusion on the ISPs' blocking database of *new* infringing servers (identified by FAPL or their contractors). Equally, this flexible formula ensures that old servers are unblocked if they stop transmitting infringing footage. By facilitating continuing input by the rightsholders, the notice and block facility enhances overall levels of effectiveness. Regular 'renewing' of the ISPs' blocking databases ensures "capture" of new infringing servers and deletion from the database of servers no longer disseminating infringing material.

Inherent Limitations Linked to Territoriality and Possible Need for Multiplicity of Proceedings

Blocking orders are, by their very nature, territorial.⁶⁶ In other words, an English webblock can only be enforced against ISPs in the jurisdiction of England and Wales. Naturally, webblocks have no extra-territorial effect. But, this fact may pose problems for rightsholders whose IPRs may be enforceable beyond the narrow confines of just one country (jurisdiction). A good example is the EU Trade Mark, granted by the EU Intellectual Property Office. This particular IPR has unitary effect, and is both valid and enforceable across the 28 country bloc of the EU. So, if counterfeit products were being sold online, in breach of an EU Trade Mark, and those counterfeit products were viewable online from (hypothetically), 7 different EU Member States, then the trade mark owner would be obliged to seek a webblocking injunction in each of the 7 countries. This lack of a pan-European blocking order forces the prejudiced IP owners to institute separate proceedings in each country and matters can be compounded by the risk that a blocking injunction may not be available in some of the seven countries affected.⁶⁷

Assuming the blocking order remedy is available in all seven countries affected, the claimant IP rightsholder has no choice but to engage in a multiplicity of proceedings.⁶⁸ On a practical note, this means undertaking considerable expense, uncertainty and consumption of valuable time/resources for the claimant rightsholder.⁶⁹ Another limitation is the fact that blocking access in 7 EU Member States to an infringing website, located say, in a non-EU country such as the Russian Federation, may have only limited effectiveness. That will be so because purchasers of the counterfeit products (living in countries *other than* the countries in which the blocks were granted) can continue to purchase the infringing products online.

⁶⁶ Kostyantyn Lobov, "The Effectiveness of Blocking Injunctions" (<https://www.harbottle.com/news/effectiveness-blocking-injunctions/>, 17 August 2016) (accessed 20th January, 2018)

⁶⁷ A good example is Germany, whose courts have taken a rather equivocal approach to webblocking injunctions for IP infringements. In fact, to this author's knowledge, no webblocking injunctions have *actually* been granted by the German courts up to now though it has to be said that two significant judgments delivered by the German *Bundesgerichtshof* (Federal Supreme Court), in November 2015, pave the way for blocking injunctions. They are: (I ZR 174 /14) (Goldesel) and, (I ZR 3/14), involving GEMA, the German Collecting Society of Musical Authors as plaintiffs. See, generally, Jaani Riordan, *The Liability of Internet Intermediaries*, (Oxford Press, 2016) at 514.

⁶⁸ Alpana Roy and Althaf Marsoof, "The blocking injunction: a comparative and critical review of the EU, Singaporean and Australian regimes" *European Intellectual Property Review*, (2016), 38 (2), 92 at 98.

⁶⁹ While each set of proceedings will feature the same (IP rightsholder) claimant, each case will have a different set of defendants, i.e. the ISPs which operate in the State in which the proceedings are instituted.

So, while a webblock order clearly has positive effect in the jurisdiction in which it is granted, its effectiveness is in fact *circumscribed* by that jurisdiction's geographic boundaries.

Some Conclusions on the criterion of Effectiveness

Like all putative remedies in an online environment, the webblock is not one hundred per cent effective. It is not a silver bullet (but, there may never be a silver bullet!). Silver bullets are often illusory and frequently unrealistic when it comes to online IP infringement prevention. Rapid technological developments are often exploited first by infringers, and only later is there “catch-up” by legitimate IP holders to counteract infringements. The technologically savvy will always find a way to circumvent a webblock but that fact should not diminish the relative usefulness and effectiveness of webblock orders. This author submits that rightsholders would long have given up on applying for webblocking orders if they were largely ineffective.⁷⁰ The creative and innovative approach of the High Court towards webblocks (e.g. *FAPL*) virtually guarantees that Sct 97A will be invoked by UK rightsholders for quite some time to come.

Looking outside the UK for evidence of effectiveness, it is worth noting that mature IP regimes such as Singapore and Australia recently adopted webblocking legislation (in 2014 and 2015, respectively) while the Swedish courts granted their first webblocking injunction in 2017. Tellingly, the German Bundesgerichtshof (Federal Supreme Court) also paved the way for webblocking injunctions when it handed down two important judgments in late-2015.⁷¹ By this author's reckoning, at least 14 European countries now offer webblocking as a remedy to IP owners and this can really only be seen as a strong endorsement of the injunction's efficacy.

At a domestic law level, webblock injunctions were made available to UK trademark owners for the first time in 2014 (by virtue of the *Cartier* ruling) and this extension of the blocking jurisdiction to trade mark cases was upheld by the Court of Appeal in 2016.⁷² At CJEU level,

⁷⁰ A key paragraph in *Cartier* is determinative when it comes to assessing the effectiveness of webblocks. In paragraph 217 of the judgment, Arnold J states “I am not persuaded that there are alternative measures open to Richemont (one of the Claimants) which would be equally effective, but less burdensome”. This is the learned judge's assessment, having carefully examined the alternatives to a webblock order, namely, actions against the operators, notice and takedown by hosts, payment freezing, domain name seizure, de-indexing and customs seizure. Analysis carried out at [198] to [216] of the ruling. In short, considering the (then) state of technological evolution, Mr Justice Arnold's view was that there were no real alternatives to blocking orders.

⁷¹ On 26 November 2015 the German Bundesgerichtshof (Federal Supreme Court) handed down two judgments (both unreported) which pave the way for blocking injunctions. The first ruling – (I ZR 174 /14) (Goldesel) featured the major companies of the German music industry as plaintiffs while the second ruling - (I ZR 3/14) featured GEMA, the German Collecting Society of Musical Authors as plaintiffs. While the Goldesel decision paves the way for a sensible webblocking possibility in Germany, based on the concept of *Storerhaftung*, two issues still need to be resolved before the first webblock is granted in Germany. Firstly, the issue of costs accruing on the ISP's side need to be balanced against the interests of the rightsholders and, secondly, the issue of exactly what action is required from rightsholders vis-à-vis the primary infringers and host service providers as a prerequisite for making the ISP's intervention reasonable. See Martin Schaefer, ‘ISP liability for blocking access to third-party infringing content’ (2016) 38 EIPR 633, 638.

⁷² *Cartier International AG v British Sky Broadcasting Limited* [2016] EWCA Civ 658.

the seminal *Telekabel* judgment⁷³ permits webblocks in the 28 Member States. Collectively, these developments confirm confidence and belief among both judges and legislatures in the webblock order *as an effective remedy*. One can only assume that this combination of confidence and belief is built on respectable and acceptable levels of webblock effectiveness.

4. The Criterion of Legitimacy

This part of the article will assess webblocking injunctions in the context of their legitimacy, to determine whether webblocking orders are legitimate, or “acceptable”..⁷⁴ Naturally, in this context, what is at issue is whether regulators are doing the correct thing by giving a positive steer (encouraging a certain type of behaviour), negative steer (*discouraging a certain type of behaviour*) or, should they adopt a neutral permissive line?⁷⁵

In the specific context of inhibiting online IP infringement, “behaviour” could actually refer to two types of behaviour, firstly, the behaviour of ISPs and secondly, the behaviour of individual internet users. By legislating for webblocks, a country’s legislature is explicitly involving ISPs (whether they like it or not) in the fight against online IP infringement. Stated less delicately, the legislature is obligating ISP cooperation through court-supervised webblocks. This more than “encourages” a certain type of behaviour. It is, in effect, *requiring* a certain type of behaviour by the ISPs, but with a worthy overarching goal in mind, i.e., the prevention (and ultimate reduction) of online IP infringement.

Legislation and case-law will be examined to determine whether the primary tool against online copyright and trade mark infringement is “legitimate”?

Legislation

From a legislative perspective, webblocking orders in the UK and the 27 other EU Member States have undoubted legitimacy. Arguably, the initial genesis of the UK webblock is to be found in Article 8 (3) of the EU Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive).⁷⁶ Article 8 (3) requires EU Member States to “ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.” Section 97A of the CDPA, 1988 (as amended), is the domestic legislative provision based on Art 8 (3) of the InfoSoc Directive.⁷⁷ Compellingly, since the

⁷³ Case C-314/12, *UPC Telekabel Wien v Constantin Film Verleih*, ECLI:EU:C:2014:192. This preliminary ruling (following a preliminary reference from the Oberster Gerichtshof, Austria) concerned a website making cinematographic works available to the public without the rightsholder’s consent. In authorising the use of open-textured webblocks throughout the EU, the CJEU made their grant subject to a test of proportionality, whereby the granting authority, whether judicial or non-judicial in nature, would be required to strike a balance between three distinct rights or freedoms. They are, firstly, copyright (intellectual property rights, generally), secondly, the freedom to conduct a business and, thirdly, the freedom of information of internet users.

⁷⁴ In other words, do the webblocking injunctions pass moral muster?, see: Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (Oxford, 2008), at 9, citing Karen Yeung, *Securing Compliance* (Oxford: Hart, 2004).

⁷⁵ Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (Oxford, 2008), at 11, citing Karen Yeung, *Securing Compliance* (Oxford: Hart, 2004).

⁷⁶ [2001] OJ L167/10.

⁷⁷ Section 97A, CDPA, was inserted into the primary Act by Regulation 27 of the Copyright and Related Rights Regulations 2003 (SI 2003/2498). Sect 97A CDPA empowers the the English High Court (and the Court of Session in Scotland) to grant a webblocking

seminal UK webblock ruling in 2011,⁷⁸ Sct 97A has been the subject of fifteen written judgments in the area of IP webblocking.⁷⁹ Moreover, over the last seven years, this provision has been invoked with increasing success by a diversity of rightsholders and has generated a rich and thoughtful series of webblock rulings.

But while *Cartier* is undoubtedly a jurisprudential milestone,⁸⁰ the judgment was achieved despite a legislative lacuna in UK domestic law. From a legitimacy perspective, one could potentially question the “pedigree” of *Cartier* as there was no specific UK statutory basis available to the High Court at the time to grant a webblock *in a trademark context*. However, the court adroitly filled this troublesome lacuna⁸¹ to ensure a level playing field for both copyright holders and trade mark holders in the UK. It did this by interpreting Section 31 of the Senior Courts Act 1981 in a broad fashion and in a way favourable to trademark holders⁸² The Court achieved this by invoking the important EU Law principle of indirect effect (the *Marleasing* principle⁸³) to ensure that the defective UK law would be interpreted *so far as it is possible* (within the limits of the *Marleasing* principle) in light of the EU Enforcement Directive.⁸⁴ By extending the UK’s webblocking jurisdiction to cover trademark

injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright.

⁷⁸ Namely, *Twentieth Century Fox v British Telecommunications Plc* [2011] EWHC 1981 (colloquially known as the Newzbin2 case).

⁷⁹ They are: *Twentieth Century Fox Film Corp v British Telecommunications plc* [2011] EWHC 1981 (Ch); [2012] Bus LR 1471; *Twentieth Century Fox Film Corp v British Telecommunications plc (No 2)* [2011] EWHC 2714 (Ch); [2012] Bus LR 1525; *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch); [2012] 3 CMLR 14; *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd (No 2)* [2012] EWHC 1152 (Ch); [2012] 3 CMLR 15; *EMI Records Ltd v British Sky Broadcasting Ltd* [2013] EWHC 379 (Ch); [2013] ECDR 8; *Football Association Premier League Ltd v British Sky Broadcasting Ltd* [2013] EWHC 2058 (Ch); [2013] ECDR 14; *Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd* [2013] EWHC 3479 (Ch); [2014] ECDR 7; *Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd* [2014] EWHC 937 (Ch); *1967 Limited v British Sky Broadcasting* [2014] EWHC 3444 (Ch); *Twentieth Century Fox Film Corporation v Sky UK Limited* [2015] EWHC 1082 (Ch); *Cartier International AG v British Sky Broadcasting Ltd* [2014] EWHC 3354 (Ch); *Cartier International AG v British Sky Broadcasting* [2016] EWCA Civ 658; *Cartier International Limited v British Telecommunications* [2016] EWHC 339 (Ch); *Football Association Premier League and Others v British Telecommunications and Others* [2017] EWHC 480 (Ch); and, *Football Association Premier League Ltd v British Telecommunications Plc* [2017] EWHC 1877 (Ch)

⁸⁰ Until the 2014 landmark judgment of *Cartier International v British Sky Broadcasting Limited*, [2014] EWHC 3354 (Ch), trademark owners were the poor relation when it came to webblock orders. But, *Cartier* changed all that. In granting a webblock order to claimant trade mark owners, the UK courts expanded the UK webblocking jurisdiction to cover online trademark infringements. By this judgment, the rights of prejudiced copyright holders and trade mark holders have been equalised when it comes to blocking orders.

⁸¹ This lacuna occurred through a failure by the UK legislature to transpose the third sentence of Article 11 of the Enforcement Directive into local law. The third sentence of Article 11 ensures that IP rightholders *in general* (not just copyright holders) are in a position to obtain (blocking) injunctions against intermediaries, whose services are used by a third party to infringe an IP right.

⁸² Section 31 provides that the High Court may by order (whether interlocutory or final) grant an injunction ... in all cases in which it appears to be just and convenient to do so.

⁸³ In essence, the *Marleasing* principle expands the law of indirect effect in two ways. Firstly, it requires all national law to be interpreted in the light of EU law, irrespective of whether it is implementing law or not and irrespective of whether it was enacted prior or subsequent to the provision of EU law in question. In *Marleasing*, the Spanish Civil Code, which concerned civil/contract law, had to be interpreted in the light of a subsequent piece of EU Company legislation. Secondly, it strengthened the national courts’ interpretive duty. See Generally: Damien Chalmers, Gareth Davies and Giorgio Monti, *European Union Law: Cases and Materials* (2nd edn, Cambridge University Press 2010) at 295. As Christopher Docksey and Barry Fitzpatrick observed ‘it is no longer sufficient for a national court to turn to Community Law only if the national provision is ambiguous. Its priority must be to establish the meaning of the Union obligation and only then to conclude whether it is possible to achieve the necessary reconciliation with the national law’ Christopher Docksey and Barry Fitzpatrick, ‘The Duty of National Courts to Interpret Provisions of National Law in Accordance with Community Law’ (1991) 20 ILJ 113. See Case C-106/89 *Marleasing SA v La Comercial Internacional de Alimentacion SA* [1990] ECR I-4135; [1992] 1 CMLR 305. ,

⁸⁴ Directive 2004/48/EC of 29th April 2004 on the enforcement of intellectual property rights [2004] OJ L157/45.

infringements, the High Court equalised the rights of copyright holders and trade mark owners. As a consequence of the ruling, now trade mark owners could avail of the popular webblock remedy. Importantly, the judgment caused UK webblocking jurisprudence to evolve in a new, albeit entirely natural and logical direction. Noteworthy too is the fact that, to this author's knowledge, no other country in the EU (with the possible exception of Denmark) has, up to now, granted a webblock order in relation to online trade mark infringement.⁸⁵

By adopting this creative approach to statutory interpretation and invoking the important *Marleasing* principle in EU Law, the High Court was able to establish a *type* of legislative legitimacy for webblock orders in the specific context of online trademark infringement, thereby overcoming the UK government's failure to transpose the third sentence of Article 11 of the Enforcement Directive into local law.

Case-law

Although the CJEU's *Telekabel* ruling 'arrives' rather late in the day, (coming a full eight years after the first ever blocking injunction, handed down in Denmark in 2006),⁸⁶ the judgment is particularly significant from a legitimacy perspective. By the CJEU approving of webblocking injunctions, it offers **legitimacy** to this particular IP remedy right across the 28-nation EU bloc. In *Telekabel*, the CJEU sets out a balancing test (a type of proportionality test), which must be satisfied for the blocking order to be acceptable in the eyes of the courts. This balancing test must be applied by entities (judicial or otherwise) which grant blocking injunctions based on Article 8(3), InfoSoc Directive. The test requires the granting body to strike a balance between three key freedoms or rights contained in the Charter of the Fundamental Rights of the EU.⁸⁷

From the perspective of the UK blocking regime, the balancing test is something that should not cause too much concern for the English courts. They are in the fortunate and happy position of having been strong proponents of proportionality pre-*Telekabel*. Given that the English courts' practice of proportionality was quite thorough, even prior to *Telekabel*, this author submits that one can assume quite safely that English webblocking judgments pass muster when it comes to the criterion of legitimacy.

A good practical example is *EMI Records Ltd v British Sky Broadcasting Ltd*⁸⁸ where Arnold J devotes a significant part of his judgment to the principle of proportionality.⁸⁹ In that ruling, Mr Justice Arnold refers back to his approach to proportionality in *Golden Eye International*

⁸⁵ See para [6] of *Cartier International AG v British Sky Broadcasting Limited*, [2014] EWHC 3354 (Ch), where Arnold J refers to a Danish case *Home A/S v Telenor A/S* (Retten på Frederiksberg, 14 December 2012) as being the only other possible case in the EU involving a website-blocking order against internet service providers in order to combat trade mark infringement.

⁸⁶ *Aller International v Tele2 A/S* (Case No. FI-15124/2006). The judgment, handed down by the Copenhagen City Court on 25th October 2006, required Tele2 to block the website www.allofmp3.com. For an English translation of the ruling: <http://copyrightblog.kluweriplaw.com/wp-content/uploads/sites/49/2015/01/allofmp3-UK.pdf>

⁸⁷ They are: the right to property and, by extension, the right to have one's IP protected (Article 17); (ii) the freedom to conduct a business, which economic agents such as ISPs enjoy under Article 16 of the Charter, and (iii) the freedom of information of internet users, whose protection is ensured by Article 11 of the Charter.

⁸⁸ [2013] EWHC 379 (Ch)

⁸⁹ The principle of proportionality is dealt with at paras [90] to [107] of the judgment.

The following can be extrapolated from *Golden Eye*. It is clear that the English High Court had already implemented a proportionality test or balancing test **prior** to the landmark *Telekabel* ruling. Compellingly, this test was also affirmed by the UK Supreme Court, two years prior to *Telekabel*.⁹¹ From a legitimacy perspective, the English courts were both *ahead of the curve* and prescient. The *Golden Eye* judgment's considered and thoughtful approach on striking a balance between key fundamental rights in *Golden Eye* shows how the English courts were satisfying the legitimacy criterion *even before Telekabel* was handed down!⁹²

The English situation stands in stark contrast with the situation in Austria pre-*Telekabel* (the *Telekabel* judgment commenced life as a preliminary reference from Austria). The Austrian

⁹⁰ [2012] EWHC 723 (Ch), In *Golden Eye*, Arnold J set out the two reasons why it is necessary to consider the proportionality of court orders in the field of intellectual property. Interestingly, both refer to EU Law. Firstly, Article 3 (2) of the Enforcement Directive imposes a general obligation to consider the proportionality of remedies for the infringement of intellectual property rights. Secondly, the CJEU has held (in a number of cases) that, when adopting measures to protect copyright owners against online infringement, national courts must strike a fair balance between the protection of intellectual property rights and the protection of the fundamental rights of individuals who are affected by such measures, and in particular the rights safeguarded by the applicable Articles of the Charter.⁹⁰ These cases are: Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-271 at [61]-[68], C-70/10 *Scarlet Extended SA v Société belge des auteurs compositeurs et éditeurs (SABAM)* [2011] ECR I-0000, [2012] ECDR 4 at [42]-[46], [50]-[53] and Case C-360/10 *Société belge des auteurs compositeurs et éditeurs (SABAM) v Netlog NV* [2012] ECR I-0000, [2012] 2 CMLR 18at [41]-[51]. As *Golden Eye* concerned a claim by copyright holders for a Norwich Pharmacal Order against one of the UK's main ISPs, the case predictably featured strong tensions between key rights held by the claimant IP holders and the alleged copyright infringers (who were in effect, subscribers to the Defendant's services). These important rights were protected by the European Convention on Human Rights and the Charter of Fundamental Rights of the EU. In terms of his approach, Mr Justice Arnold adopted a logical first step and set out the rights engaged by the case (at [117]). They were : property/intellectual property rights⁹⁰ the right to privacy⁹⁰ and the right to the protection of personal data.⁹⁰ The first set of rights enumerated accrue to the copyright holders whilst the second and third sets accrue to the individual subscribers to the ISP's services. The next step, - **striking the balance** between the three various sets of rights – would involve four distinct elements. They are as follows: (i) neither right as such has precedence over the other; (ii) where the **values** under the two rights are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary; (iii) the justifications for interfering with or restricting each right must be taken into account; (iv) finally, the proportionality test – or 'ultimate balancing test' - must be applied to each."

⁹¹ This occurred in *Rugby Football Union v Viagogo Ltd*, [2012] UKSC 55. The Defendant Appellant, Consolidated Information Services (formerly Viagogo Ltd) was a third party ticketing website. The RFU (the Claimant Respondent) had a deliberate policy of allocating tickets at low prices to grassroots organisations to develop the game and enhance its popularity. The claim was brought in respect of tickets for matches in 2010 and 2011 which the RFU alleged Viagogo had permitted to be anonymously advertised and sold on its website at prices above face value. The RFU alleged that any sale of its tickets above face value would constitute a breach of contract, rendering the ticket null and void. Arguing that Viagogo had become mixed up in the wrongdoing, the RFU sought a NPO against Viagogo, requiring it to identify those advertising and selling the tickets, as well as the details of the tickets themselves. In rejecting the appeal, the Supreme Court stated that the ultimate balancing test set out by Lord Steyn in *In re S* [2005] 1 AC 593 is also applicable to the balancing of different rights under the Charter of the Fundamental Rights of the EU. The Court also confirmed that it is a correct statement of how to approach proportionality in relation to NPOs. Most notable in terms of the approach to be taken to Norwich Pharmacal applications, is the extent to which the proportionality of granting such an order can be influenced by 'big picture' considerations as to its ultimate purpose. These are inevitably fact specific, but an indication of their potential extent can be derived from the fact that the RFU in this appeal aimed to protect its interest in the promotion and development of rugby as a sport.

⁹² In terms of his approach, Mr Justice Arnold adopted a logical first step and set out the rights engaged by the case (at [117]). They were : property/intellectual property rights⁹² the right to privacy⁹² and the right to the protection of personal data.⁹² The first set of rights enumerated accrue to the copyright holders whilst the second and third sets accrue to the individual subscribers to the ISP's services. The next step, - **striking the balance** between the three various sets of rights – would involve four distinct elements. They are as follows: (i) neither right as such has precedence over the other; (ii) where the **values** under the two rights are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary; (iii) the justifications for interfering with or restricting each right must be taken into account; (iv) finally, the proportionality test – or 'ultimate balancing test' - must be applied to each."

courts were not particularly diligent when it came to balancing the fundamental rights of the parties involved in litigation and Arnold J does not shy away from making this point in *EMI Records*.⁹³ In *Telekabel*, for instance, the claimants had applied for a general "prohibition of outcome", i.e. an absolute bar on the ISP "facilitating access" to the infringing website.⁹⁴ And while a "prohibition of outcome" was a standard order under the Austrian law relating to infringements of absolute rights, its granting by a court would not involve any balancing test of the fundamental rights of the parties involved. Drawing a conclusion, therefore, using the two comparators – the UK webblocking regime and, the Austrian webblocking regime, pre-*Telekabel*, the former was considerably better prepared and equipped to don the mantle of legitimacy post-*Telekabel*, thanks to its established balancing of fundamental rights approach, an approach that was ultimately endorsed by the UK's highest court in *Rugby Football Union v Viagogo Ltd*⁹⁵, a full two years prior to *Telekabel*.

Moreover, the pre-*Telekabel* period was marked by significant inconsistency among EU Member States on the point of the proportionality of blocking orders. There was a call for the matter of webblocking applications to be judged in a uniform manner throughout Europe in accordance with CJEU guidelines for assessing the proportionality of specific blocking measures. But, Arnold J's statements in *EMI Records* that "the proportionality of a blocking order is bound to be a context-sensitive question"⁹⁶ and that the High Court does not make such orders without thorough consideration of whether it is appropriate to make an order in the light of the specific facts of each case,⁹⁷ speaks volumes about how far down the road of legitimacy the English courts had (already) travelled.

While *Telekabel* unquestionably bestows legitimacy *at international level* on the webblock remedy, it is worth looking at the contrast between the CJEU's judgment and the Advocate General's Opinion in the case to see where the limits of legitimacy in this context now lie. The controversial aspect of *Telekabel* can be summed up by the important difference of opinion within the EU's Judiciary (broadly defined) as to the nature and character of the webblock order. The author posits that this internal "debate" within the EU's judicial organ in no way undermines the legitimacy of the webblock, but yet it highlights two contrasting viewpoints, one *prescriptive in nature*, the other more *permissive*, on the type of webblock order to be granted.

The difference of opinion occurred when the CJEU decided not to follow Advocate-General Cruz Villalon on the important point of the nature or character of the webblock order.⁹⁸ In its

⁹³ *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch) at [96]

⁹⁴ *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch) at [96]

⁹⁵ [2012] UKSC 55, [2012] 1 WLR 3333 at [45].

⁹⁶ *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch) at [100]

⁹⁷ In this regard, Mr Justice Arnold refers specifically to three High Court rulings, namely, *Twentieth Century Fox Film Corp v British Telecommunications plc* [2011] EWHC 1981 (Ch); *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd (No 2)* [2012] EWHC 1152 (Ch) and, *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch).

⁹⁸ As the court follows the Advocate-General's Opinion in about ninety per cent of cases, this divergence of opinion would have been, at the very least, a talking point.

judgment, the CJEU stated that a blocking injunction could be legitimate even if it does not specify the actual blocking measures that an ISP must take.⁹⁹

This contrasts markedly with the Advocate General who stated that the blocking injunction should specify the measures to be taken by the ISP as that was appropriate for the protection of the rightsholder's copyright.¹⁰⁰ This less flexible injunction was preferred by the Advocate General for two reasons, both of which relate to the infringement side of the equation. Firstly, Internet users can circumvent the blocking measure without major difficulty and, secondly, the operators of the copyright-infringing website can provide the page in identical form under a different IP address and domain name.¹⁰¹

This author submits that these two reasons point to the need for *more, not less* flexibility to be given to the ISP. If the blocking measures are specified in the injunction, that restricts the ISP's room for manoeuvre, and potentially reduces the likelihood of a creative approach to the problem. Additionally, this less flexible injunction may leave the ISP somewhat hamstrung when it comes to countering rapidly changing IP addresses/domain names.

At first sight, this open-textured injunction specified by the CJEU in *Telekabel* seems to benefit the addressee ISP. Subject to the 2 provisos enumerated by the court, the ISP appears to be afforded considerable latitude in terms of which measures it takes to block. But, upon closer scrutiny, the CJEU's judgment in *Telekabel* may actually put ISPs in a quandary as follows: an open-textured or generic injunction may leave the ISP in the somewhat unhappy position of having to guess what the court actually has in mind. Where the blocking measures are not specified by the court, it is up to the ISP to decide whether domain name or IP address blocking (or a combination of both) needs to be effected. It also needs to decide the degree or level of the blocking, a challenging issue as the ISP must try and strike the correct balance between the key elements of effectiveness, extensiveness, intrusiveness and expense.

A mis-assessment by the ISP, which could involve *underblocking or overblocking* will likely provoke fresh litigation by either the rightsholder or, general internet users. If an ISP were to mis-gauge the three key Charter freedoms/rights specified by the CJEU in *Telekabel*, it might end up re-appearing as defendant before the very court that held against it in the first place! This is not the ideal outcome from either a PR or reputational perspective!

Where a court declines to spell out specific blocking measures in its order, then there is always the risk that the ISP will not really understand what is reasonable/unreasonable, from the perspective of the law. The ISP may well opt for a mild blocking measure (in the interests of freedom of information) or, a more severe blocking measure (to protect the rightsholder's IP) but both options carry risks. A mild blocking measure may fail to seriously discourage infringers, potentially causing the ISP to be penalised by the court. A more severe blocking measure may just cause serious disagreements between the ISP and its customers. Having

⁹⁹ Case C-314/12, *UPC Telekabel v Constantin Film and Wega Filmproduktionsgesellschaft*, at [52]

¹⁰⁰ Case C-314/12, *UPC Telekabel v Constantin Film and Wega Filmproduktionsgesellschaft*, Opinion of AG Cruz Villalon, para 90 and 102.

¹⁰¹ Case C-314/12, *UPC Telekabel v Constantin Film and Wega Filmproduktionsgesellschaft*, Opinion of AG Cruz Villalon, para 99.

the possibility to defend itself in the enforcement process is of little real consolation to the ISP. Nor does it alter or reduce the ISP's dilemma.

From the viewpoint of legitimacy, both the CJEU and its Advocate General *legitimate* webblocking injunctions. But, clearly, the CJEU's approach is *permissive* while the Advocate General's is *prescriptive*. Importantly, neither approach undermines the legitimacy of webblocking orders *but*, somewhat ironically, both approaches create challenges for the addressee ISP. The specific webblock, favoured by the Advocate General, affords the ISP little room for manoeuvre, something most ISPs would not welcome, given the rapid changes in technology. In addition, the less flexible, specific webblock order might leave the ISP 'hamstrung' when it comes to counteracting strategies deployed by the operators of infringing websites or streaming servers. A good example includes the frequent changing of the IP address or domain name, from which they are operating, so as to counteract video monitoring technologies¹⁰² used by rightsholders. As for the generic or open textured webblock, favoured by the CJEU, they, almost counterintuitively, also create difficulties for ISPs. Without real or effective guidance from the granting body (whether judicial or administrative), the ISP must make important decisions about the type and level of web or streaming server blocking to implement. In addition, it is in the unenviable position of having to strike the correct balance between the key elements of effectiveness, extensiveness, intrusiveness and expense. While it is unfortunate that the permissive and prescriptive approaches adopted by the Court and Advocate General, respectively, have their weaknesses, neither 'dilutes' the core legitimacy bestowed on webblocking orders generally. On a pragmatic note, as the CJEU 'overruled' its Advocate General in *Telekabel*, generic webblocks have now been approved by the EU's highest court.

Conclusions on Legitimacy

In analysing whether webblock orders fulfil the criterion of legitimacy, the author examined the webblock from two different perspectives, - legislative and, jurisprudential. In both contexts, the legitimacy criterion was fulfilled, though slight caveats have to be added in each case.

From a legislative perspective, webblocking orders in the UK and the 27 other EU Member States (for that matter) have unquestioned legitimacy, that legitimacy deriving from Article 8 (3) of the InfoSoc Directive. The UK transposed the all important Article 8 (3) into local law by way of Section 97A, CDPA (1988) and this particular provision has generated all of the copyright-related webblock rulings in the UK to date. Therefore, demarcating between copyright webblocks and trademark webblocks for a moment, there is nothing to impugn the legitimacy of the former but a question mark (of sorts) hangs over the latter.

¹⁰² These video monitoring technologies enable IP rightsholders to identify infringing internet streams with a high level of accuracy in close to real time. They are referred to in the *FAPL v BT* judgment.

The question mark arises due to the obvious legislative *lacuna* in UK domestic law, existing just before the watershed *Cartier* ruling. The failure of the UK government to transpose the third sentence of Article 11 of the Enforcement Directive theoretically left UK trademark in quite a perilous position. As it so happened, Arnold J. adroitly succeeded in filling the lacuna through a combination of broad statutory interpretation and, the invocation of the *Marleasing* principle. But the cynic might argue that the embarrassing legislative *lacuna* would have put pressure on Mr Justice Arnold to find a practical solution. Undoubtedly, UK trade mark owners were clamouring for their own equivalent of Sct 97A, CDPA, as they looked enviously at the webblock orders granted to their friends in the copyright community. But, in having to rely on Sct 31 of the Senior Courts Act and the *Marleasing* principle, Arnold J was falling back on *non-specific* UK legislation and a principle on conforming interpretation. While the author concedes that *a type* of legislative legitimacy is created for UK trade mark webblocks through the *Cartier* judgment, it is, in a way, judge-made legitimacy!

From the perspective of legitimacy, *Telekabel* is of particular importance. The supremacy of EU Law over domestic law is clearly a compelling factor but the main significance comes from the approval granted by the CJEU to webblocks, subject to a balancing test being conducted by the granting court/administrative organ. This balancing test refers to three rights contained in the Charter of Fundamental Rights of the EU. These rights protect IP ownership, the freedom to conduct a business and, the freedom of internet users.

An examination of UK case-law, handed down pre-*Telekabel* is instructive. From this, it is very evident that the principle of proportionality was well established and applied by the British courts, **pre-Telekabel**. The principle is very prominent in *EMI Records Ltd v British Sky Broadcasting Ltd*¹⁰³ but was also well ventilated in the prior rulings, - *Golden Eye* and, *Rugby Football Union v Viagogo*. Clearly, the English courts were both ahead of the curve and prescient in terms of proportionality.¹⁰⁴ And, given that the principle of proportionality (and striking the correct balance between various fundamental rights) was a major condition in *Telekabel*, one can only deduce that the UK webblock judgments were, for all intents and purposes, **legitimate even before** the balancing test was ‘mandated’ by the CJEU in *Telekabel*.

5. General Conclusions

In this article, the author has critically evaluated the primary ‘weapon’ of IP rightsholders against two key concerns or criteria: effectiveness and, legitimacy. Besides being the principal ‘weapon’ of rightsholders, the webblocking order is also, contemporaneously, the main regulatory intervention tool in the context of online copyright infringement in quite a number of countries in the world. *Cartier* demonstrates that the webblock order now offers significant potential to trade mark owners and this novel and unique UK judgment may yet provide considerable inspiration to other countries’ judiciaries and legislatures in terms of expanding the scope of webblocking orders beyond ‘mere’ copyright infringement. This

¹⁰³ [2013] EWHC 379 (Ch)

¹⁰⁴ The conclusion that the English courts were a lot more advanced than some of their Continental counterparts when it came to striking the correct balance, was further amplified by Arnold J’s useful analysis of the situation in Austria (pre-*Telekabel*), in *EMI Records*. See: *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch) at [96]

article demonstrates that the English High Court and, Court of Appeal have, together, become a type of lodestar in terms of webblocking orders. The High Court has consistently delivered innovative and forward-thinking webblocking judgments, as exemplified in the recent *FAPL* ruling, where the High Court granted a blocking order against illegal *streaming servers*, as opposed to illegal websites. In *FAPL*, the Court crafted its Order around new technologies used by *both* the Claimant and the Defendant. In addition, the Court accommodated the notice and block approach to make the blocking process as flexible and effective as possible. This judicial dexterity augurs well for twenty first century rightsholders in the UK and will, in all likelihood, act as a compelling ‘template’ for courts in other jurisdictions. The webblocking zeitgeist is well and truly captured by the English courts, with a powerful mantra of “novelty” resonating in the background.

As regards effectiveness, this article proves that webblocking orders are the most effective regulatory intervention at the moment. In many regards, they are superior to the alternative measures/interventions available and this was stated clearly by Arnold J in *Cartier*. The author concedes that the webblock order is not a silver bullet but there may never be a silver bullet for online IP infringements. The technology is evolving so fast that it negates the possibility of a silver bullet. When it comes to the academic commentators surveyed, most of them are positively disposed to webblocking orders and even those that are somewhat lukewarm in their views, concede that the webblock is, at the very least, a pragmatic solution.

Empirical research from the U.S. is compelling too as it shows unequivocally that webblocking is effective along four different planes: a reduction in the number of visits to blocked websites, a decrease in total piracy, an increase in visits to paid legal streaming sites and, an increase in videos viewed on legal ad-supported streaming sites.

As imitation is the sincerest form of flattery, the UK’s webblocking regime must be doing something right! Over the past four years, two of the world’s most significant IP ‘players’, Australia and Singapore, have adopted webblocking legislation. In addition, the Swedish courts granted their first webblocking injunction last year, while in late-2015, the German Bundesgerichtshof (Federal Supreme Court) paved the way for webblocking injunctions when it handed down two important judgments in late-2015. In *Telekabel*, the CJEU approved open textured webblock orders. Clearly, this approval from the EU’s highest court, which has resonance in all 28 Member States, is built on a belief and confidence in the webblock as an effective IP remedy. In this author’s estimation, there are now at least 25 countries in the world (14 of them European) offering the webblock order as a possible remedy to their IP rightsholders. These important **global** developments, both legislative and jurisprudential, are strong and unmistakeable endorsements of the effectiveness of the webblocking order.

In assessing how legitimate webblocking orders are, the author carried out his evaluation by looking at legislation and case-law. As regards UK legislation, the author’s analysis was two-pronged, to cover legislative provisions covering, firstly, copyright-related webblocks and,

secondly, trademark-related webblocks. In terms of the former, the finding was that copyright-related webblocks have undoubted legitimacy in the UK, by virtue of Sct 97A, CDPA. Since the seminal UK webblocking ruling in 2011, in *Twentieth Century Fox v British Telecommunications*, Sct 97A has been the basis of fifteen written senior court judgments, almost all of which have been handed down by the High Court. Impressive too is the breadth of rightsholders that have relied on Sct 97A to protect their IPRs. Unsurprisingly, music and movie copyrightholders feature prominently on the list of Sct 97A claimants but, blocking orders have also been sought by (and granted to) eBook owners and, the owner of television broadcasting rights (i.e. FAPL). Clearly, a *de jure* and *de facto* legitimacy has developed in and around *copyright* webblocks.

A finding of undoubted legislative legitimacy for copyright webblocks contrasts with a finding of questionable legislative legitimacy for trademark webblocks in the UK. A legislative lacuna lies at the heart of the somewhat flawed legislative legitimacy for trademarks. While the author fully acknowledges Arnold J's adroit handling of the dilemma through deft use of statutory interpretation and, the *Marleasing* principle, it does not fully remove some niggling doubts about the legislative legitimacy of trademark webblocks in the UK. The solution provided was a judge-made one, necessitated by a misstep by the government in its reading and interpretation of Art 11 of the Enforcement Directive.

The 2014 CJEU ruling in *Telekabel* is the cornerstone of the analysis of legitimacy, from a case-law perspective. Not only is it the seminal webblocking judgment from the EU's highest court, but it also gives the imprimatur to domestic courts (or administrative bodies) in the 28 Member States to grant webblocking injunctions so long as they comply with a balancing test relating to three key rights contained in the Charter of Fundamental Rights of the EU. The author's examination of senior court rulings in the UK, *pre-Telekabel*, demonstrates that the British courts were, even then, very advanced, comparatively speaking, in their thinking on the principle of proportionality. Lastly, a 'contretemps' between the CJEU and its Advocate General about the *type* of blocking order that should be granted - prescriptive (specific measures) or permissive (open textured) - does not, in any way, undermine the legitimacy of webblocking orders. It just reflects two different philosophical approaches about the role and function of the granting court and/or the addressees of the court order, i.e. the ISPs.

*** **